anand guru

SOC EXPERTS

Interview Questions on **Security Concepts**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is CIA?

Confidentiality, **Integrity** and **Availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security.

Component	Definition	How do you ensure?
Confidentiality	Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals.	Encryption Access Control
Integrity	Ensuring the data is not modified either in transit or at storage.	Hashing
Availability	Ensuring the systems and data is readily available to its users.	Redundancy Backups Load Balancers

anand guru

What is Encryption? Explain types of encryption.

Encryption is the process of encoding information in such a way that only authorized parties can understand it.

Encryption is done using Keys.

There are 2 types of Encryption:

- **Symmetric Encryption** - Same key is used for encryption and decryption.
  - E.g.: Blowfish, AES, RC4, DES, RC5, and RC6
- **Asymmetric Encryption** - Different keys are used encryption and decryption.
  - E.g.: RSA, DSA, Elliptic curve techniques, PKCS.

anand guru

Explain Asymmetric Encryption.

In asymmetric encryption different keys are used encryption and decryption.

Typically know as Private Key and Public Key (also referred to as Key Pair).

Any data encrypted with public key can only be decrypted by the corresponding private key.

Example:

- A server keeps a key-pair. The public key is issued to all the users who request a connection.
- At the user's end, the application encrypts the data using the server provided public key.
- Once the encrypted message reach the server, the server decrypts the message using its private key.

anand guru

What is Hashing?

- Hashing is the transformation of a string of characters into a fixed-length value or key that represents the original string.

- Hashing is one-way. i.e. it is not possible to get the data back from the hash value.
- Hashing is used to ensure the integrity of the data.

E.g.:

- MD5 - 32 Hexadecimal characters
- SHA-1 - 40 Hexadecimal characters
- SHA-256 - 64 Hexadecimal characters

anand guru

Explain difference between Encryption and Hashing.

Encryption	Hashing
Encryption is the process of encoding information in such a way that only authorized parties can understand it.	Hashing is the transformation of a string of characters into a fixed-length value or key that represents the original string.
Two-way. i.e. we can get the data back by decryption	One-way. i.e. we cannot get the data back from hash value
Used to ensure confidentiality	Used to ensure integrity
Algorithms: AES, DES, Bluefish	Algorithms: MD5, SHA-1, SHA-256

anand guru

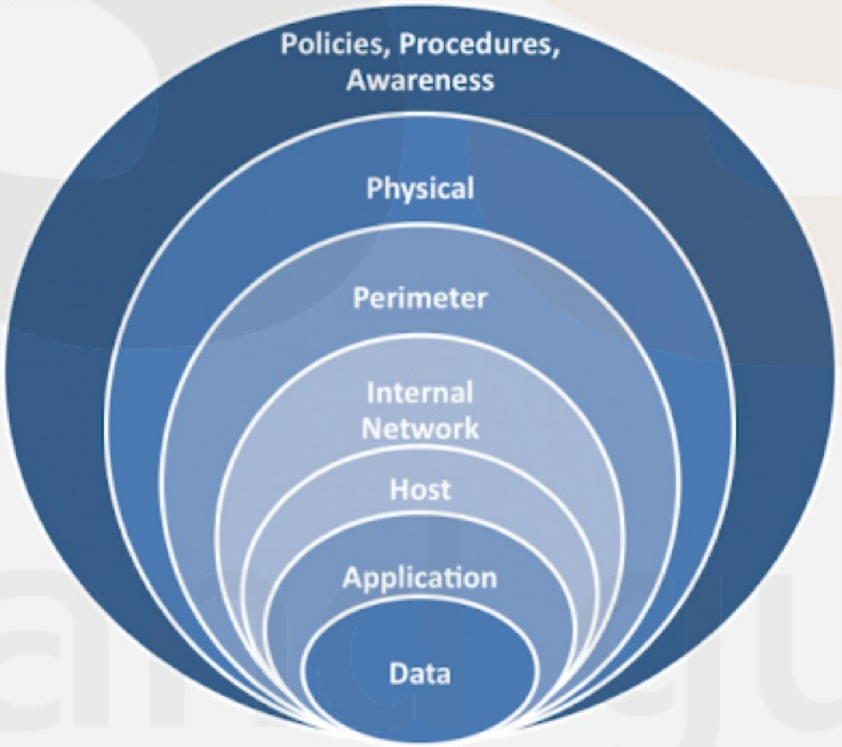
What is Vulnerability, Risk, Threat and Exploit?

Vulnerability	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.
Risk	The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
Threat	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
Exploit	The tool or mechanism used to take advantage of the vulnerability

anand guru

Explain Defense in Depth.

- Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information.
- If one mechanism fails, another steps up immediately to thwart an attack.
- This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.



anand guru

What is System Hardening?

Systems hardening is a process of securing a system by reducing its attack surface.

Few things on the system hardening checklist include:

- Changing the default user credentials
- Closing all unused ports
- Stopping all unused services
- Install updates and patches
- Implement Access Control
- Install Antivirus and keep the signatures up-to-date

anand guru

What is Zero Trust Model.

Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Few principles of zero trust model are:

- Assume there are attackers both inside and outside the network
- Concept of least privilege
- Use Multi Factor Authentication wherever possible.

anand guru

Explain Kerberos.

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow systems to prove their identity to one another in a secure manner.

Here are the most basic steps taken to authenticate in a Kerberized environment.

1. Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC)
2. The KDC verifies the credentials and sends back an encrypted TGT and session key
3. The TGT is encrypted using the Ticket Granting Service (TGS) secret key
4. The client stores the TGT and when it expires the local session manager will request another TGT (this process is transparent to the user)

If the Client is requesting access to a service or other resource on the network, this is the process:

5. The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
6. The KDC verifies the TGT of the user and that the user has access to the service
7. TGS sends a valid session key for the service to the client
8. Client forwards the session key to the service to prove the user has access, and the service grants access.

anand guru

If budget is not a concern how do you secure a web server?

If budget is not a concern a web server can be secured by deploying the following technologies

Network Security

- Anti-DDOS technology
- Firewall (To block traffic on unnecessary ports)
- Intrusion Prevention System
- Web Application Firewall

Host Security

- Antivirus
- HIPS/Host Firewall
- Application control (To restrict the processes running)

Apart from these preventive technologies, we should implement System Hardening and also enable log monitoring on the Web servers.

Also, the web application should be thoroughly tested by application penetration testing methods.

anand guru

What do you understand by compliance in Cybersecurity?

A compliance framework is a structured set of guidelines that details an organization's processes for maintaining its cyber security.

There are industry specific compliances like:

PCI-DSS – To protect credit card data. (Banks and E-commerce)

HIPAA – To protect patients health information. (Hospitals and Insurance companies)

SOX – Public listed companies

GDPR – European companies and business that run in European countries.

anand guru

Hackers and their motivation

Different types of Hackers

- **White Hat Hackers**
  - White hat hackers are authorized hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity.
- **Black Hat Hackers**
  - Black Hat Hackers are hackers who hack for malicious intentions. Like financial gains.
- **Grey Hat Hackers**
  - Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain.
- **Script Kiddie**
  - A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers.
- **Hacktivist**
  - Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.
- **State/Nation Sponsored Hackers**
  - State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country.
- **Malicious Insider or Whistleblower**
  - A malicious insider or a whistleblower could be an employee of a company or a government agency who gains access/knowledge of inside operations which he speculates to be illegal and threatens to go public.

Few Random questions.

If you had to both compress and encrypt data during a transmission, which would you do first?

- Compress first (to reduce the size) and then Encrypt. Encryption on more data will take longer time.

Between TLS and SSL, which is more secure?

- TLS. SSL is the predecessor of TLS

What is Zeroday?

- A vulnerability or a malware that has be identified but doesn't have a fix (patch or signature) yet. It is the time period between a vulnerability/malware being identified and release of patch/signature.

Difference between VA and PT.

- Vulnerability Assessment is a process of identifying the vulnerabilities in a system or network.

Penetration Testing is to go one step ahead of identifying the vulnerabilities and exploit the vulnerability.

anand guru